The Virginia Joint Commission

JCOTS

on Technology and Science

Cyber Security Advisory Committee

Tuesday, October 16, 2012 10:00 a.m.

Speaker's Conference Room, 6th Floor, General Assembly Building

The second meeting of the Cyber Security Advisory Committee of the Joint Commission on Technology and Science was held on October 16, 2012. Advisory Committee member, Delegate Tom Rust (chairman), was present, as well as citizen members from the private sector, local governments, and the Commonwealth's institutions of higher education were present and actively participated in the Committee discussions.

After Delegate Rust called the meeting to order, the Advisory Committee received four presentations. Sam Nixon, Chief Information Officer, and Sam Nixon, Chief Information Security Officer, both of VITA, gave an overview of cyber security within the Commonwealth. Prior to the creation of VITA, each of the Commonwealth's government agencies had its own IT team. This led to duplicative systems, obstacles to sharing data, and inadequate security. Since its creation in 2003 VITA has centralized Virginia's IT services and has transitioned 86 out of 89 agencies to the new services. The three agencies that have not transitioned to VITA prefer to remain autonomous.

VITA is tasked with security governance of all three branches of Virginia's government. It controls the infrastructure, while agencies remain responsible for application management. Agencies must comply with VITA's policies and standards which include security controls for data protection. VITA's data protection efforts include conducting intrusion detection and vulnerability scanning, providing software patching, and encrypting email.

The Commonwealth has been the target of over 70 million attacks in a six month period. In that same time frame, over 320 million spam messages were detected. The attacks originate from around the world. VITA has seen an increase in security incidents in the last 2 years. Going forward, VITA plans to upgrade its infrastructure, to add capability to analyze network traffic, and to increase its mobile device security. The Advisory Committee was concerned with the challenges VITA faces. Members discussed the balance between VITA's authority to ensure compliance and its accountability for security breaches.

Leslie Fuentes, Director of Information Technology for the City of Hampton, gave a brief overview of Virginia's Operational Integration Cyber Center of Excellence

(VOICCE) program. VOICCE was created with a grant from the Department of Homeland Security. While the grant has expired, VOICCE created a cyber lab and conducts exercises in partnership with Thomas Nelson Community College.

Ms. Fuentes noted that local governments are particularly vulnerable to cyber attacks. VITA has no authority to set standards for local governments. The Advisory Committee noted that this was particularly troubling because local government systems are linked to state systems. Adversaries target a system's weakest link and could be targeting local government systems as a gateway to the broader state network. The Committee discussed setting state standards for local government and how the state and local government could increase collaboration on standards.

Bradford Willke, Cyber Security Advisor from the Department of Homeland Security, gave a presentation on cyber security partnerships. Mr. Willke noted that the sophistication of cyber attacks continues to increase. Targeted attacks are becoming more common. DHS works with state and local governments to identify and secure vulnerable systems.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a partnership between several state and local governments. MS-ISAC is a "911" like system for cyber incidents. It provides cyber incident coordination, handling, and response. as well as system ("Albert") for threat monitoring, detection, and prevention that is based on the Federal system ("Einstein"). MS-ISAC also provides low cost annual cyber security awareness and training.

In 2011, the Department of Homeland Security conducted the Nationwide Cyber Security Review (NCSR). The NCSR was a study to measure the effectiveness of security control placement based on risk management processes. The DHS received responses from entities in 49 out of 50. While the majority of respondents have adopted cyber security control frameworks, these frameworks are under tested and have not been upgraded. The Advisory Committee asked Mr. Willke what could be done to improve cyber security. Mr. Willke noted that defenses should be threat agnostic, and that testing should be conducted under imperfect conditions as attacks don't occur in a controlled setting.

Dr. T Charles Clancy, Director of the Hume Center for National Security and Technology out of Virginia Tech, gave a presentation on ideas for cyber security leadership by the Commonwealth. Dr. Clancy purposed that VRS dedicate a portion of its funds to investing in cyber security companies. He noted that the New York pension fund had achieved a 30% return while on funds dedicated to cyber security companies. Dr. Clancy also advocated for incentives for private entities to secure their critical cyber infrastructure.

Following the presentations and discussion, Delegate Rust asked the Committee members about their willingness to continue the discussion. The consensus was that the

Advisory Committee should continue into next interim. Delegate Rust then called on the members each create a list of cyber security challenges and the direction the Committee should take going forward.

The meeting was adjourned.